Lectures dirigées – Nombres constructibles

Giovanni Lebaron & Taddéo Rocq, sous la direction d'Antoine Dequay

ENS Rennes – Année universitaire 2023–2024

Table des matières

1 Le corps des nombres constructibles **3**
- 1.1 Définitions de base . . . 3
- 1.2 Repère orthonormé . . . 3
- 1.3 Constructions élémentaires . . . 4
- 1.4 Opérations sur les nombres constructibles . . . 6

2 Caractérisation des réels constructibles **7**
- 2.1 Quelques rappels sur les corps . . . 7
  - 2.1.1 Extensions de corps . . . 7
  - 2.1.2 Extensions successives . . . 7
  - 2.1.3 Polynôme minimal . . . 7
- 2.2 Le résultat de Wantzel . . . 7
- 2.3 Réponses aux problèmes . . . 10
- 2.4 Étude de la réciproque . . . 10

3 Le théorème de Gauss **12**
- 3.1 Angles orientés . . . 12
- 3.2 Caractérisation des angles trisectables . . . 12
- 3.3 Deux lemmes essentiels . . . 13
- 3.4 Rappels sur les polynômes cyclotomiques et les racines de l'unité . . . 14
- 3.5 Nombres de Fermat et constructibilité des polygones réguliers . . . 15

4 Compléments **19**
- 4.1 Extension aux nombres complexes . . . 19
- 4.2 Construction par neusis . . . 19
- 4.3 Vers la théorie de Galois . . . 22
  - 4.3.1 Quelques définitions . . . 22
  - 4.3.2 Correspondances entre sous-groupes et sous-corps . . . 22
  - 4.3.3 Extensions normales et théorème de Galois . . . 23
  - 4.3.4 Retour au problème des polygones réguliers . . . 23
  - 4.3.5 Nouvelle démonstration du théorème de Gauss . . . 23

Introduction

Les mathématiques de la Grèce antique furent d'une importance considérable dans l'histoire de la discipline. Avec elles sont en effet apparus les fondements du raisonnement mathématique et de la géométrie. Trois grands problèmes dans ce domaine furent posés par des mathématiciens de l'époque :

- la duplication du cube : est-il possible de construire un cube ayant pour volume deux fois celui d'un cube quelconque à la règle non graduée et au compas ?
- la trisection de l'angle : est-il possible de sectionner en trois parties égales un angle quelconque ?
- la quadrature du cercle : est-il possible de construire un carré de même aire qu'un disque quelconque ?

À ces trois problèmes s'ajoute parfois celui de la construction des polygones réguliers à la règle et au compas. Pour être résolus, ces problèmes demandaient de traduire la notion de constructibilité géométrique en des propriétés algébriques, mais ils étaient en apparence si simples que les recherches d'amateurs se sont multipliées à partir du XVIII$^{\text{ème}}$ siècle. L'Académie des Sciences de Paris prend alors en 1775 une décision radicale :

> « L'Académie a pris, cette année, la résolution de ne plus examiner aucune solution des problèmes de la duplication du cube, de la trisection de l'angle ou de la quadrature du cercle ».

C'est en 1837 que Pierre-Laurent Wantzel (1814–1848) publie une démonstration rigoureuse d'un théorème général qui entraîne l'impossibilité de la duplication du cube et de la trisection de l'angle [Wan37], puis en 1882, Ferdinand von Lindemann (1852–1939) démontre la transcendance de π, enterrant définitivement la possibilité d'une quadrature du cercle exacte [Lin82]. Nous allons tenter d'explorer cette notion de constructibilité à travers une démarche algébrique, puis nous étudierons quelques polygones réguliers et tenterons de caractériser ceux qui sont constructibles.

1 Le corps des nombres constructibles

1.1 Définitions de base

On se donne une partie finie $\mathcal{B}$ du plan euclidien $\mathcal{P} = \mathbb{R}^2$ dont les éléments seront appelés *points de base*. Intuitivement, on veut qu'un point soit qualifié de « constructible » si on peut l'atteindre uniquement :

- en traçant à la règle *non graduée* la droite passant par deux points de $\mathcal{B}$;
- en traçant au compas le cercle centré en un point de $\mathcal{B}$, de rayon la distance entre deux points de $\mathcal{B}$.

Si $A, B \in \mathcal{P}$, on notera (AB) la droite passant par A et B. Si $A \in \mathcal{P}$ et $r \geq 0$, on notera $\mathrm{C}(A, r)$ le cercle de centre A et de rayon r. On appellera tous ces lieux géométriques des *cercles-droites*. On notera enfin AB la distance euclidienne entre A et B.

Définition 1.1. *Soit $M \in \mathcal{P}$. On dit que M est* constructible à partir de $\mathcal{B}$ *lorsqu'il existe des points $M_1, \ldots, M_{n-1}, M_n \in \mathcal{P}$ tels que $M_1 \in \mathcal{B}$, $M_n = M$, et pour tout $i \in \{2, \ldots, n\}$, M_i est l'intersection de deux cercles-droites distincts, de la forme $(M_{a_i} M_{b_i})$ ou $\mathrm{C}(M_{a_i}, |M_{b_i} - M_{c_i}|)$ avec $a_i, b_i, c_i \in \{1, \ldots, i-1\}$.*

Dans les sections 1 et 2, nous supposerons que $\mathcal{B} = \{O, I\}$. Nous verrons que deux points de base sont amplement suffisants pour réaliser beaucoup de constructions. Dans ce cas et pour simplifier, l'expression « constructible à partir de $\mathcal{B}$ » sera abrégée en « constructible » dans toute la suite.

Définition 1.2. *Soient $A, B \in \mathcal{P}$. La droite (AB) est dite* constructible *lorsque A et B le sont.*

Définition 1.3. *Soient $A \in \mathcal{P}$ et $r \geq 0$. Le cercle $\mathrm{C}(A, r)$ est dit* constructible *lorsque A l'est, et que r est la distance entre deux points qui le sont.*

Par exemple, la droite (OI) et le cercle $\mathrm{C}(O, OI)$ sont constructibles. Nous allons déjà nous servir de cela pour construire un repère orthonormé, et produire diverses constructions géométriques de base.

1.2 Repère orthonormé

Commençons par tracer le cercle $\Gamma = \mathrm{C}(O, OI)$. Ce dernier coupe la droite (OI) en un point I' de l'axe (Ox). Les cercles $\mathrm{C}(I, II')$ et $\mathrm{C}(I', II)$ se coupent alors en deux points K et L. Notons que seul K est représenté sur la figure ci-dessous, L étant son symétrique par rapport à O.

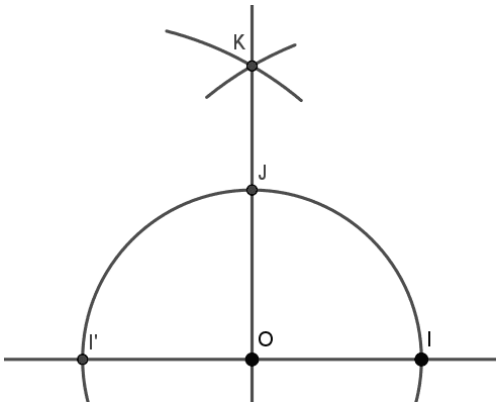


FIGURE 1 – Construction d'un repère orthonormé.

En particulier, $KI = KI' = LI = LI'$ donc K et L appartiennent à la médiatrice du segment $[II']$. Ainsi, la droite (KL) coupe Γ en un point J, qui est aligné avec les points O et K. Puisque $J \in \Gamma$, on a bien $OJ = 1$, donc (O, I, J) est un repère orthonormé de $\mathcal{P}$.

On peut désormais repérer les points par leurs coordonnées, et le repère (O, I, J) fournit une orientation pour les longueurs. On notera $\overline{AB}$ la distance algébrique entre les points A et B dans ce repère, sachant que $\overline{OI} = 1$.

1.3 Constructions élémentaires

Nous allons voir qu'il est possible, à l'aide de la règle non graduée et du compas seulement, d'effectuer les constructions géométriques de base dans le plan : perpendiculaires, parallèles, milieux, médiatrices, etc.

Proposition 1.4. *Si A et B sont deux points constructibles distincts, alors le milieu et la médiatrice du segment $[AB]$ sont constructibles.*

Démonstration. Les cercles $\mathrm{C}(A, AB)$ et $\mathrm{C}(B, AB)$ se coupent en deux points P et Q. La droite (PQ) est alors la médiatrice du segment $[AB]$, et le milieu M de $[AB]$ n'est autre que l'intersection de (AB) avec (PQ). □

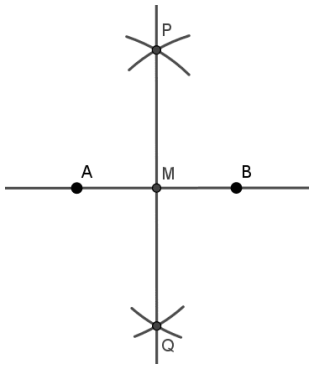


FIGURE 2 – Construction d'une médiatrice et d'un milieu.

Proposition 1.5. *Si D est une droite constructible et A est un point constructible, alors la perpendiculaire et la parallèle à D passant par A sont constructibles.*

Démonstration. Puisque D est constructible, elle contient deux points constructibles distincts P et Q. Supposons tout d'abord A et P distincts. Le cercle $\mathrm{C}(A, AP)$ coupe $D = (PQ)$ en un point R, qui est bien distinct de P car $A \neq P$, donc $\mathrm{C}(A, AP) \neq \{A\}$. Comme dans la construction précédente, on trace les cercles $\mathrm{C}(P, PR)$ et $\mathrm{C}(R, PR)$, qui se coupent en deux points B et C (seul B est représenté sur la figure ci-dessous).

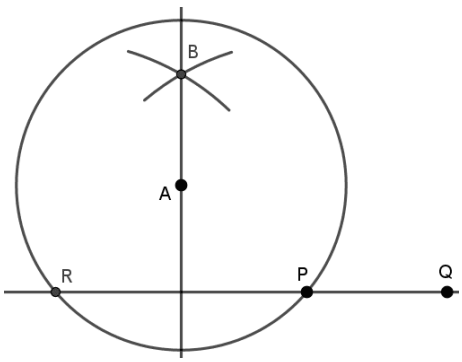


FIGURE 3 – Construction d'une perpendiculaire.

La droite (AB) est alors la perpendiculaire à D passant par A, puisque A et B appartiennent à la médiatrice du segment $[PR]$. Celle-ci est bien constructible d'après la proposition 1.4. En particulier, $P \notin (AB)$. Si A et P sont confondus, on effectue la même construction en remplaçant P par Q. Pour construire la parallèle à D passant par A, on applique deux fois le résultat précédent. □

Proposition 1.6. *Soient D et D' deux droites constructibles non parallèles. Alors la bissectrice de l'angle formé par D et D' est constructible.*

Démonstration. On note A le point d'intersection de D et D'. Le cercle $\mathrm{C}(A, r)$, par exemple pour $r = OI = 1$, coupe D en un point P et D' en un point P'. Les cercles $\mathrm{C}(P, r)$ et $\mathrm{C}(P', r)$ se coupent alors en un point Q, distinct de A. La droite (AQ) est l'une des bissectrices cherchées. □

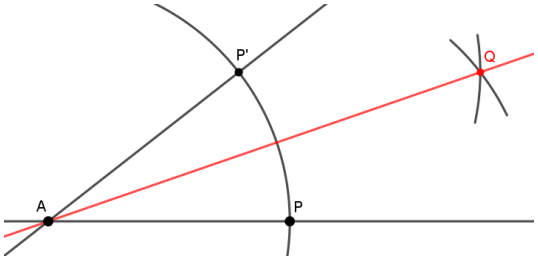


FIGURE 4 – Construction d'une bissectrice.

Définition 1.7. *Soit $t \in \mathbb{R}$. On dit que t est* constructible *lorsque c'est l'une des coordonnées d'un point constructible dans le repère orthonormé (O, I, J).*

Proposition 1.8. *Soit $t \in \mathbb{R}$. Alors t est constructible si, et seulement si, le point de coordonnées $(t, 0)$ est constructible (si, et seulement si, le point de coordonnées $(0, t)$ l'est).*

Démonstration. Supposons que t soit constructible. Par définition, t est donc l'une des coordonnées d'un point constructible M. On note A et B les projections orthogonales de M sur chacun des axes, qui sont bien constructibles d'après la proposition 1.5. Si t est l'abscisse de M, alors c'est aussi l'abscisse de A et c'est terminé. Si t est l'ordonnée de M, alors c'est l'ordonnée de B, qu'on peut le reporter sur (Ox) pour obtenir le point C comme ci-dessous, qui est l'intersection de (OA) et $\mathrm{C}(O, OB)$. En particulier, t est l'abscisse de C. La réciproque et l'équivalence avec la troisième assertion sont évidentes. □

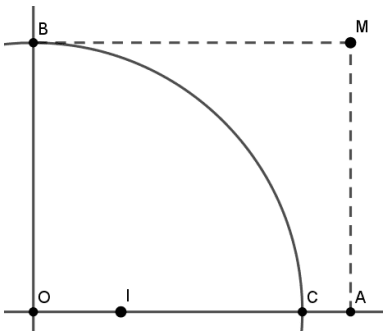


FIGURE 5 – Construction des projetés orthogonaux.

Proposition 1.9. *Si A est un point constructible et x est un réel constructible, alors le cercle $\mathrm{C}(A, |x|)$ est constructible.*

Démonstration. D'après la proposition 1.8, on peut construire le point M de l'axe (Ox) d'abscisse x, et il est alors clair que $\mathrm{C}(A, |x|) = \mathrm{C}(A, OM)$. □

1.4 Opérations sur les nombres constructibles

On note $\mathscr{C}_\mathcal{B}$ l'ensemble des nombres réels constructibles à partir de $\mathcal{B}$, ou simplement $\mathscr{C}$ lorsque $\mathcal{B} = \{O, I\}$. Intuitivement, en reportant avec le compas la longueur OI sur l'axe (Ox), on obtient déjà $\mathbb{Z} \subseteq \mathscr{C}$. Toute la question est de savoir quels points on peut atteindre avec les deux outils à notre disposition.

Théorème 1.10. *L'ensemble $\mathscr{C}$ est un sous-corps de $\mathbb{R}$ stable par racine carrée.*

Démonstration. On sait déjà que 0 et 1 sont constructibles. Soient à présent $u, v \in \mathscr{C}$. On notera A le point de l'axe (Ox) d'abscisse u, qui est bien constructible d'après la proposition 1.8.

Opposé. On constate sans difficulté que $-u$ est l'abscisse de l'un des deux points d'intersection de $\mathrm{C}(O, OA)$ et (OA), l'autre ayant pour abscisse u.

Somme. On note B le point de l'axe (Ox) tel que $\overline{AB} = v$, qui est bien constructible à l'aide de $\mathrm{C}(A, |v|)$ d'après la proposition 1.9. On constate alors que $u + v$ est l'abscisse du point B.

Produit. On suppose $uv \neq 0$, sinon il n'y a rien à faire. On note B le point de l'axe (Oy) d'ordonnée v. La parallèle à (IB) passant par A coupe l'axe (Oy) en un point K. Le théorème de Thalès donne alors :

$$\frac{OB}{OK} = \frac{OI}{OA}$$

ce qui entraîne :

$$OK = OB \times OA = uv.$$

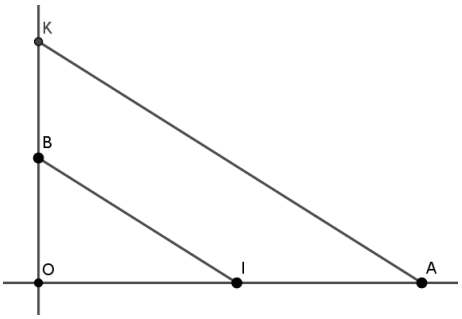


FIGURE 6 – Construction du produit.

Inverse. On suppose $u \neq 0$. La parallèle à (AJ) passant par I coupe l'axe (Oy) en un point L, et d'après le théorème de Thalès :

$$\frac{OL}{OJ} = \frac{OI}{OA}$$

ce qui entraîne :

$$OL = \frac{1}{u}.$$

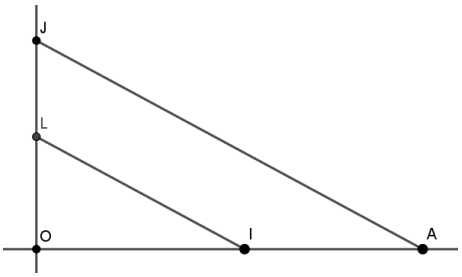


FIGURE 7 – Construction de l'inverse.

Racine carrée. On suppose $u > 0$. Soient :

- A' le point de l'axe (Ox) tel que $IA' = |u|$,
- M le milieu de $[OA']$,
- K le point d'intersection entre $\mathrm{C}(M, OM)$ et la perpendiculaire à (Ox) passant par I.

Le triangle IKM est rectangle en I, donc d'après le théorème de Pythagore :

$$IK^2 = KM^2 - IM^2 = \left(\frac{u+1}{2}\right)^2 - \left(\frac{u-1}{2}\right)^2$$

c'est-à-dire $IK^2 = u$, d'où $IK = \sqrt{u}$. □

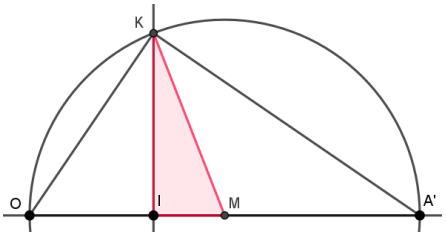


FIGURE 8 – Construction de la racine carrée.

2 Caractérisation des réels constructibles

2.1 Quelques rappels sur les corps

2.1.1 Extensions de corps

Soient K et L deux corps quelconques. On dit que L est une *extension* de K lorsque K est (ou s'identifie à) un sous-corps de L, ce que l'on note L/K. Pour $a_1, \dots, a_n \in L$, on note $K(a_1, \dots, a_n)$ le plus petit sous-corps de L contenant K et $a_1, \dots, a_n$, et on l'appelle sous-corps de L *engendré* par $a_1, \dots, a_n$. Par exemple :

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \quad ; \quad \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\} \quad ; \quad \mathbb{R}(i) = \mathbb{C}.$$

Si L est une extension de K, l'addition et la multiplication dans L munissent naturellement L d'une structure d'espace vectoriel sur K. On appelle alors *degré* de L sur K le nombre :

$$[L : K] = \dim_K(L)$$

éventuellement infini. Lorsque ce degré vaut 2, on dit que L est une extension *quadratique* de K. Pour revenir aux exemples ci-dessus, $\mathbb{Q}(\sqrt{2})$ est une extension quadratique de $\mathbb{Q}$ car $(1, \sqrt{2})$ est une base de $\mathbb{Q}(\sqrt{2})$ sur $\mathbb{Q}$.

2.1.2 Extensions successives

Soient M/L et L/K des extensions de corps. Si $(e_i)_{i\in I}$ est une base de L sur K, et $(f_j)_{j\in J}$ est une base de M sur L, alors $(e_i f_j)_{(i,j)\in I\times J}$ est une base de M sur K, d'où l'égalité :

$$[M : K] = [M : L]\,[L : K]\,.$$

Si $K_1, \dots, K_n$ sont des corps tels que chaque K_i est une extension de K_{i-1}, on parlera de *tour d'extensions* et on dira que K_n est le *sommet* de cette tour. Enfin, si chaque extension K_i/K_{i-1} est quadratique, l'égalité ci-dessus donne immédiatement $[K_n : K_1] = 2^{n-1}$.

2.1.3 Polynôme minimal

Soient L/K une extension de corps et $a \in L$. On dit que a est *algébrique* sur K lorsqu'il existe $P \in K[X] \setminus \{0\}$ tel que $P(a) = 0$. Dans le cas contraire, on dit que a est *transcendant* sur K. Si a est algébrique sur K, il existe un unique $\mu_{a,K} \in K[X]$ unitaire, irréductible sur K, tel que $\mu_{a,K}(a) = 0$. Ce dernier est appelé *polynôme minimal* de a sur K. Par exemple, $a = \sqrt{2}$ est algébrique sur $\mathbb{Q}$ et :

$$\mu_{a,\mathbb{Q}} = X^2 - 2 \quad ; \quad \mu_{a,\mathbb{R}} = X - \sqrt{2}.$$

Si $\deg(\mu_{a,K}) = n$, alors $(1, a, \dots, a^{n-1})$ est une base de $K(a)$ sur K, et donc $[K(a) : K] = n$. On dit alors que a est de *degré* n sur K. En fait, a est algébrique sur K si, et seulement si, $K(a)$ est de dimension finie sur K.

2.2 Le résultat de Wantzel

Si l'on cherche à caractériser les points constructibles par leurs propriétés algébriques, il nous faut étudier les équations vérifiées par les coordonnées de ces derniers. Ceci motive les deux lemmes suivants.

Lemme 2.1. *Soient $A(a_1, a_2), B(b_1, b_2) \in \mathcal{P}$. Alors (AB) a une équation de la forme :*

$$\alpha x + \beta y + \gamma = 0$$

avec $\alpha, \beta, \gamma \in \mathbb{Q}(a_1, a_2, b_1, b_2)$.

Démonstration. Si $a_1 = b_1$, alors (AB) a pour équation $x - a_1 = 0$. Sinon, si $x, y \in \mathbb{R}$, alors $(x, y) \in (AB)$ si, et seulement si :

$$\frac{y - a_2}{x - a_1} = \frac{b_2 - a_2}{b_1 - a_1}$$

ce qui, après simplification, montre que (AB) a pour équation :

$$\underbrace{(a_2 - b_2)}_{\alpha} x + \underbrace{(b_1 - a_1)}_{\beta} y + \underbrace{a_1(b_2 - a_2) + a_2(b_2 - a_1)}_{\gamma} = 0$$

et il est clair que $\alpha, \beta, \gamma \in \mathbb{Q}(a_1, a_2, b_1, b_2)$. □

Lemme 2.2. *Soient $A(a_1, a_2), B(b_1, b_2), C(c_1, c_2) \in \mathcal{P}$. Alors $\mathrm{C}(A, BC)$ a une équation de la forme :*

$$x^2 + y^2 + \alpha x + \beta y + \gamma = 0$$

avec $\alpha, \beta, \gamma \in \mathbb{Q}(a_1, a_2, b_1, b_2, c_1, c_2)$.

Démonstration. On sait que $\mathrm{C}(A, BC)$ a pour équation :

$$(x - a_1)^2 + (y - a_2)^2 = BC^2 = (b_1 - c_1)^2 + (b_2 - c_2)^2.$$

On constate en développant qu'elle est de la forme :

$$x^2 - 2xa_1 + a_1^2 + y^2 - 2a_2 y + a_2^2 = \delta \in \mathbb{Q}(b_1, b_2, c_1, c_2)$$

et, comme précédemment, les autres coefficients sont bien dans $\mathbb{Q}(a_1, a_2, b_1, b_2, c_1, c_2)$. □

Ces deux résultats expriment donc le fait qu'avec la règle non graduée et le compas, on ne fait apparaître que des opérations élémentaires (somme, différence, produit, quotient) et des racines carrées, via des équations de degré 1 ou 2, que l'on sait facilement résoudre. C'est l'idée directrice de la démonstration du théorème suivant.

Théorème 2.3 (Wantzel, 1837). *Soit $t \in \mathbb{R}$. Alors t est constructible si, et seulement s'il existe une tour d'extensions quadratiques $L_1 \subseteq \ldots \subseteq L_n$ telles que $L_1 = \mathbb{Q}$, $L_n \subseteq \mathbb{R}$, et $t \in L_n$.*

Démonstration. Supposons que t soit constructible, et notons $M_1(x_1, y_1), \ldots, M_n(x_n, y_n) = M(t, 0)$ la suite des points permettant de construire M. Quitte à échanger M_1 et M_2, on suppose que $M_1 = O$ et $M_2 = I$. On définit enfin les extensions successives :

$$\begin{aligned} L_1 &= \mathbb{Q}(x_1, y_1), \\ L_2 &= \mathbb{Q}(x_1, x_2, y_1, y_2), \\ &\vdots \\ L_n &= \mathbb{Q}(x_1, \ldots, x_n, y_1, \ldots, y_n). \end{aligned}$$

Il est clair que $L_1 = L_2 = \mathbb{Q}$ (car $x_1 = y_1 = y_2 = 0$ et $x_2 = 1$), que $L_1 \subseteq \ldots \subseteq L_n$, et que $t = x_n \in L_n$. Nous allons montrer que $[L_{i+1} : L_i] \in \{1, 2\}$ pour tout $i \in \{1, \ldots, n\}$, c'est-à-dire $L_{i+1} = L_i$ ou bien L_{i+1} est une extension quadratique de L_i. Supposons $i \geq 2$ et étudions le point M_{i+1}. Nous noterons $(x, y) = (x_{i+1}, y_{i+1})$.

Deux droites. Si M_{i+1} est le point d'intersection de deux droites distinctes, alors d'après le lemme 2.1, il existe $\alpha_1, \alpha_2, \beta_1, \beta_2, \gamma_1, \gamma_2 \in \mathbb{Q}(x_1, \ldots, x_i, y_1, \ldots, y_i) = L_i$ tels que :

$$\begin{cases} \alpha_1 x + \beta_1 y + \gamma_1 = 0, \\ \alpha_2 x + \beta_2 y + \gamma_2 = 0. \end{cases}$$

Les deux droites étant supposées distinctes, on peut inverser le système[1] et on en déduit :

$$\begin{pmatrix} x \\ y \end{pmatrix} = \frac{1}{\alpha_1\beta_2 - \alpha_2\beta_1} \begin{pmatrix} \beta_1\gamma_2 - \beta_2\gamma_1 \\ \alpha_2\gamma_1 - \alpha_1\gamma_2 \end{pmatrix}$$

[1] Formellement, si D et D' désignent ces deux droites, ce sont des hyperplans affines de la forme $D = \ker\varphi + \omega$ et $D' = \ker\varphi' + \omega'$ où et φ et φ' sont des formes linéaires non nulles. Plus précisément, si (e_1, e_2) désigne la base canonique de $\mathbb{R}^2$ alors $\varphi = \alpha_1 e_1^* + \beta_1 e_2^*$ et $\varphi' = \alpha_2 e_1^* + \beta_2 e_2^*$. Comme D et D' sont distinctes, (φ, φ') est libre, sinon on aurait $\varphi' = \lambda\varphi$ avec $\lambda \neq 0$, ce qui est impossible, car D et D' ne sont pas parallèles. Par conséquent, $\det(\varphi, \varphi') = \alpha_1\beta_2 - \alpha_2\beta_1 \neq 0$.

ce qui montre que $x, y \in L_i$. Par conséquent, $L_{i+1} = L_i(x, y) = L_i$.

Un cercle et une droite. Si M_{i+1} est un point d'intersection d'un cercle et d'une droite, alors d'après les lemmes 2.1 et 2.2, il existe $\alpha_1, \alpha_2, \beta_1, \beta_2, \gamma_1, \gamma_2 \in L_i$ tels que :

$$\begin{cases} \alpha_1 x + \beta_1 y + \gamma_1 = 0, & (1) \\ x^2 + y^2 + \alpha_2 x + \beta_2 y + \gamma_2 = 0. & (2) \end{cases}$$

Supposons dans un premier temps $\beta_1 \neq 0$. Alors l'égalité (1) permet d'exprimer y en fonction de x :

$$y = -\frac{1}{\beta_1}(\alpha_1 x + \gamma_1).$$

Si $x \in L_i$, alors $y \in L_i$ et comme précédemment, $L_{i+1} = L_i$. Sinon, en reportant dans (2), on obtient :

$$x^2 + \frac{1}{\beta_1^2}(\alpha_1 x + \gamma_1)^2 + \alpha_2 x - \frac{\beta_2}{\beta_1}(\alpha_1 x + \gamma_1) + \gamma_2 = 0.$$

On observe que x est solution d'une équation de la forme $\alpha x^2 + \beta x + \gamma = 0$ avec $\alpha, \beta, \gamma \in L_i$ et :

$$\alpha = 1 + \frac{\alpha_1^2}{\beta_1^2} > 0.$$

En particulier, $\alpha \neq 0$ donc x est algébrique sur L_i de degré 2. Ainsi, $[L_{i+1} : L_i] = [L_i(x) : L_i] = 2$. Maintenant, si $\beta_1 = 0$, alors $\alpha_1 \neq 0$ (équation d'une droite en dimension 2), et on reproduit la même démarche. On obtient alors une équation similaire en y, et ceci entraîne $L_{i+1} = L_i$ ou bien $[L_{i+1} : L_i] = [L_i(y) : L_i] = 2$.

Deux cercles. Si M_{i+1} est un point d'intersection de deux cercles, alors comme précédemment, d'après le lemme 2.2, il existe $\alpha_1, \alpha_2, \beta_1, \beta_2, \gamma_1, \gamma_2 \in L_i$ tels que :

$$\begin{cases} x^2 + y^2 + \alpha_1 x + \beta_1 y + \gamma_1 = 0, \\ x^2 + y^2 + \alpha_2 x + \beta_2 y + \gamma_2 = 0. \end{cases}$$

Ce système est équivalent au suivant :

$$\begin{cases} x^2 + y^2 + \alpha_1 x + \beta_1 y + \gamma_1 = 0 \\ (\alpha_1 - \alpha_2)x + (\beta_1 - \beta_2)y + \gamma_1 - \gamma_2 = 0 \end{cases}$$

On est alors ramenés au cas d'un cercle et d'une droite. Dans tous les cas, on a bien $[L_{i+1} : L_i] \in \{1, 2\}$ pour tout i. On peut alors retirer les L_i tels que $L_i = L_{i-1}$, et on obtient bien une tour d'extensions quadratiques partant de $\mathbb{Q}$ et dont le sommet contient t.

Réciproquement, supposons qu'il existe une tour d'extensions quadratiques $\mathbb{Q} = L_1 \subseteq \ldots \subseteq L_n$ avec $t \in L_n$. Montrons par récurrence que chaque L_i est contenu dans $\mathscr{C}$. Il n'y a rien à faire lorsque $i = 1$. Si maintenant $L_i \subseteq \mathscr{C}$ pour un certain $i \in \{1, \ldots, n-1\}$, considérons $x \in L_{i+1}$. Comme $[L_{i+1} : L_i] = 2$, la famille $(1, x, x^2)$ est liée sur L_{i+1}, donc il existe $(\alpha, \beta, \gamma) \in L_i^3 \setminus \{0\}$ tel que $\alpha x^2 + \beta x + \gamma = 0$. Donc si $\alpha = 0$, alors $\beta \neq 0$ et :

$$x = -\frac{\gamma}{\beta} \in L_i \subseteq \mathscr{C}.$$

Sinon, x est racine du polynôme réel $\alpha X^2 + \beta X + \gamma$, ce qui permet d'écrire[2] :

$$x = \frac{-\beta \pm \sqrt{\beta^2 - 4\alpha\gamma}}{2\alpha}.$$

Or, $\alpha, \beta, \gamma \in L_i \subseteq \mathscr{C}$ par hypothèse de récurrence, et d'après le théorème 1.10, $\mathscr{C}$ est un corps stable par racine carrée, donc $x \in \mathscr{C}$. Ceci valant pour tout $x \in L_{i+1}$, on en déduit $L_{i+1} \subseteq \mathscr{C}$. En particulier, $x \in L_n \subseteq \mathscr{C}$. □

[2] Comme ce polynôme a une racine réelle, son discriminant $\beta^2 - 4\alpha\gamma$ est bien positif, d'où l'existence de sa racine carrée.

Corollaire 2.4. *Si t est un réel constructible, alors t est algébrique sur $\mathbb{Q}$ et le degré du polynôme minimal de t est une puissance de 2.*

Démonstration. D'après le théorème de Wantzel, il existe une tour d'extensions quadratiques $L_1 \subseteq \ldots \subseteq L_n$ avec $L_1 = \mathbb{Q}$ et $t \in L_n$. Par conséquent (cf. section 2.1), $[L_n : \mathbb{Q}] = 2^{n-1}$. Par ailleurs, $\mathbb{Q} \subseteq \mathbb{Q}(t) \subseteq L_n$ donc :

$$[L_n : \mathbb{Q}] = [L_n : \mathbb{Q}(t)]\,[\mathbb{Q}(t) : \mathbb{Q}]$$

ce qui assure que $[\mathbb{Q}(t) : \mathbb{Q}]$ est fini, et c'est un diviseur de 2^{n-1} donc une puissance de 2. □

Nous appellerons ce corollaire le *résultat de Wantzel*. Il permet déjà d'éliminer une bonne partie des nombres réels dans la classification des nombres constructibles : si un nombre est transcendant sur $\mathbb{Q}$, ou si le degré de son polynôme minimal n'est pas une puissance de 2, alors il n'est pas constructible. Ce résultat nous renseigne également sur le cardinal de $\mathscr{C}$. L'ensemble $\mathbb{A}$ des réels algébriques sur $\mathbb{Q}$ est en effet dénombrable :

$$\mathbb{A} = \bigcup_{P \in \mathbb{Q}[X] \setminus \{0\}} \{x \in \mathbb{R} \mid P(x) = 0\}$$

et d'après le résultat de Wantzel, $\mathscr{C} \subseteq A$. Nous avons déjà vu que $\mathbb{N} \subseteq \mathscr{C}$, donc $|\mathscr{C}| = \aleph_0$.

Théorème 2.5. *L'ensemble $\mathscr{C}$ est le plus petit sous-corps de $\mathbb{R}$ stable par racine carrée.*

Démonstration. D'après le théorème 1.10, il suffit de montrer que si K est un sous-corps de $\mathbb{R}$ stable par racine carrée, alors $\mathscr{C} \subseteq K$. Soit $t \in \mathscr{C}$. On introduit de nouveau la tour d'extensions quadratiques obtenue par le théorème de Wantzel : $\mathbb{Q} = L_1 \subseteq \ldots \subseteq L_n \subseteq \mathbb{R}$ avec $t \in L_n$. On montre par récurrence sur $i \in \{1, \ldots, n\}$ que $L_i \subseteq K$, ce qui entraînera que $t \in K$. L'initialisation est évidente, car tout sous-corps de $\mathbb{R}$ contient $\mathbb{Q}$. L'hérédité est analogue au sens réciproque dans le théorème de Wantzel, en remplaçant $\mathscr{C}$ par K. □

Ce résultat montre qu'on obtient tous les nombres constructibles en partant de 0 et 1, via les opérations de somme, différence, produit, quotient et racine carrée. On dit que $\mathscr{C}$ est la *clôture quadratique* de $\mathbb{Q}$ dans $\mathbb{R}$.

2.3 Réponses aux problèmes

Le résultat de Wantzel permet d'ores et déjà de conclure sur les trois problèmes mentionnés en introduction. La construction des polygones réguliers sera abordée dans la section suivante.

Duplication du cube. Supposons construite l'arête d'un cube quelconque, d'extrémités que l'on nommera O et I, ce qui permet de reproduire les constructions précédentes. Doubler le volume de ce cube revient à multiplier la longueur du segment $[OI]$, égale à 1 dans le repère (O, I, J), par $\sqrt[3]{2}$. Il est en effet annulé par $P = X^3 - 2$, et c'est son polynôme minimal puisque P est scindé à racines simples sur $\mathbb{C}$ et ses racines sont irrationnelles. Comme il est de degré 3, il est irréductible. La duplication du cube est donc impossible.[3]

Quadrature du cercle. Supposons construit un disque quelconque de centre O, et considérons un point I de son bord. Son aire vaut donc π dans le repère (O, I, J). Le côté d'un carré de même aire a donc nécessairement pour longueur $\sqrt{\pi}$. Ce nombre n'est pas constructible car sinon, π le serait, mais il est transcendant.

Trisection de l'angle. Nous montrerons dans la section suivante qu'il n'existe aucune méthode générale pour trisecter un angle quelconque, et nous donnerons une caractérisation des angles trisectables.

2.4 Étude de la réciproque

On peut se demander si le résultat de Wantzel est une équivalence, à savoir, si un réel est algébrique sur $\mathbb{Q}$ et son degré est une puissance de 2, est-il constructible ? Nous allons y répondre par la négative, en montrant que

[3] Le critère d'Eisenstein assure que $X^n - 2$ est irréductible sur $\mathbb{Q}$ pour tout $n \geq 2$. En toute généralité, la duplication de l'hypercube en dimension n est donc possible si, et seulement si, n est une puissance de 2.

le polynôme $P = X^4 - X - 1$ est irréductible sur $\mathbb{Q}$ et possède une racine réelle non constructible. Comme il est de degré 4, on peut déjà le factoriser dans $\mathbb{R}[X]$ comme suit :

$$\begin{aligned} P &= \underbrace{\left(X^2 + aX + b\right)}_{\stackrel{\text{def}}{=} P_1}\underbrace{\left(X^2 + cX + d\right)}_{\stackrel{\text{def}}{=} P_2} \\ &= X^4 + (a+c)X^3 + (ac + b + d)X^2 + (ad + bc)X + bd. \end{aligned}$$

En identifiant les coefficients, on en déduit :

$$\begin{cases} a + c = 0, \\ ac + b + d = 0, \\ ad + bc = 1, \\ bd = -1, \end{cases}$$

c'est-à-dire :

$$\begin{cases} a = -c, & (1) \\ b + d = a^2, & (2) \\ a(b - d) = 1, & (3) \\ bd = -1. & (4) \end{cases}$$

On déduit de (2) et (4) que b et d sont les racines de $X^2 - a^2X - 1$. On peut également supposer d'après (1) que $a > 0$ (et donc $c < 0$), puisque (3) assure que $a \neq 0$. Cette même équation assure également que $b > d$, on peut donc les expliciter via la formule quadratique :

$$b = \frac{a^2 + \sqrt{a^4 + 4a^2}}{2} \quad ; \quad d = \frac{a^2 - \sqrt{a^4 + 4a^2}}{2}$$

On déduit enfin de (1) l'égalité :

$$a(b - d) = a\sqrt{a^4 + 4a^2}$$

ce qui donne :

$$a^2\left(a^4 + 4a^2\right) = a^6 + 4a^4 = 1.$$

Donc a^2 est racine de $B = X^3 + 4X^2 - 1$. Pour montrer que c'est bien son polynôme minimal sur $\mathbb{Q}$, il suffit de montrer qu'il n'a pas de racine rationnelle, car B est unitaire et de degré 3. Or, s'il existe $p/q \in \mathbb{Q}$, avec p et q premiers entre eux, tel que $B(p/q) = 0$, alors :

$$a^3 + 4ab^2 = b^3$$

donc a divise b^3. Enfin, a et b étant premiers entre eux, a et b^3 également, donc $a = b = 1$, mais $B(1) \neq 0$. Contradiction. Donc B est irréductible sur $\mathbb{Q}$. Comme son degré n'est pas une puissance de 2, a^2 n'est pas constructible d'après le résultat de Wantzel, donc a non plus.

Examinons maintenant les racines de P_1 et P_2. Notant Δ_1 et Δ_2 leurs discriminants respectifs, on a alors :

$$\Delta_1 = a^2 - 4b = -a^2 - 2\sqrt{a^4 + 4a^2} < 0$$

donc P_1 possède deux racines complexes conjuguées. De plus, comme $a > 0$:

$$\Delta_2 = c^2 - 4d = -a^2 + 2\sqrt{a^4 + 4a^2} > 0$$

donc P_2 possède deux racines réelles distinctes α et β. On constate que $\alpha + \beta = -c = a$, et comme a n'est pas constructible, α ou β ne l'est pas non plus.

Il reste à vérifier que P est irréductible dans $\mathbb{Q}[X]$. Puisque $a \notin \mathscr{C}$, le résultat de Wantzel assure que $a \notin \mathbb{Q}$. Par conséquent, la décomposition $P = P_1P_2$, unique dans $\mathbb{R}[X]$, ne peut avoir lieu dans $\mathbb{Q}[X]$.

3 Le théorème de Gauss

3.1 Angles orientés

Pour essayer de caractériser les polygones réguliers constructibles, il est nécessaire de faire appel à quelques outils supplémentaires, nécessitant d'utiliser désormais des angles orientés. Le repère orthonormé (O, I, J) défini précédemment oriente le plan. On notera $\Gamma = \mathrm{C}(O, OI)$ et Γ^+ l'ensemble des points de Γ d'ordonnée positive.

Définition 3.1. *Soit $\theta \in \mathbb{R}$. On note $\widehat{\theta}$ l'angle orienté dont θ est une mesure, et on dit que cet angle est* constructible *lorsque le point $M \in \Gamma$ tel que $(\overrightarrow{OI}, \overrightarrow{OM}) = \widehat{\theta}$ est constructible.*

Proposition 3.2. *Si $\theta \in \mathbb{R}$, alors $\widehat{\theta}$ est constructible si, et seulement si, $\cos\theta \in \mathscr{C}$.*

Démonstration. Si $\widehat{\theta}$ est constructible, le point $M \in \Gamma$ tel que $(\overrightarrow{OI}, \overrightarrow{OM}) = \widehat{\theta}$ est constructible. Sa projection sur l'axe (Ox) l'est donc également, et elle a pour abscisse $\cos\theta$. Réciproquement, si $\cos\theta$ est constructible, on peut construire le point H tel que $\overline{OH} = \cos\theta$. On peut ensuite construire la perpendiculaire à l'axe des abscisses passant par H. Cette dernière coupe Γ en deux points, et l'un d'entre eux est le point M cherché. □

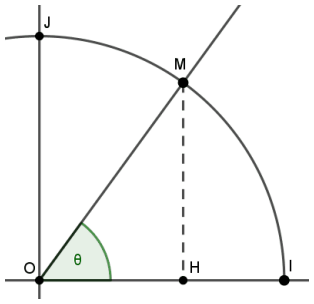


FIGURE 9 – Construction de $\cos\theta$ à partir de θ.

3.2 Caractérisation des angles trisectables

Définition 3.3. *Soit $\theta \in \mathbb{R}$. On dit que θ est* trisectable *lorsque le point $N \in \Gamma^+$ tel que l'angle $\widehat{ION}$ ait pour mesure $\theta/3$ est constructible.*

Cette définition revient donc à dire que $\cos(\theta/3)$ est un nombre réel constructible à partir de $\mathcal{B} = \{O, I, M\}$.

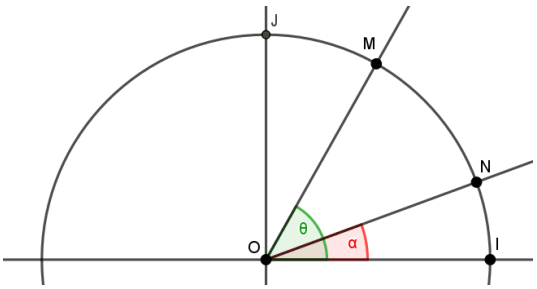


FIGURE 10 – Représentation des angles θ et $\alpha = \theta/3$.

Pour montrer que la trisection de l'angle est *en général* impossible, il suffit par exemple de montrer qu'un angle de mesure $\pi/3$ n'est pas trisectable. Pour ce faire, nous allons une nouvelle fois utiliser le résultat de Wantzel.

Rappelons tout d'abord l'identité, valable pour tout $\theta \in \mathbb{R}$:

$$\cos\theta = 4\cos^3\left(\frac{\theta}{3}\right) - 3\cos\left(\frac{\theta}{3}\right)$$

qui montre que $\cos(\pi/9)$ est racine de $P = 8X^3 - 6X - 1$. Montrons que P n'a pas de racine dans $\mathbb{Q}$.

Supposons par l'absurde qu'il existe $p/q \in \mathbb{Q}$, avec p et q premiers entre eux, tel que $P(p/q) = 0$. Alors :

$$8p^3 = 6pq^2 + q^3.$$

En particulier, p divise q^3 et q^2 divise $8p^3$. Comme p et q sont premiers entre eux, on en déduit $p \in \{-1, 1\}$, puis $q \in \{-2, -1, 1, 2\}$. On vérifie facilement que dans tous les cas, $P(p/q) \neq 0$. Contradiction. Puisque P est de degré 3, il est donc irréductible sur $\mathbb{Q}$. Ainsi, $\cos(\pi/9)$ est algébrique et son polynôme minimal est $P/8$, ce qui montre que $\cos(\pi/9)$ n'est pas constructible.

Avant de continuer, précisons que l'on a ajouté le point M à $\mathcal{B}$. Les résultats obtenus avec deux points de base se généralisent en fait sans difficulté si $\mathcal{B}$ contient, outre O et I, d'autres points $A_1(x_1, y_1), \ldots, A_p(x_p, y_p) \in \mathcal{P}$:

- $\mathscr{C}_\mathcal{B}$ est le plus petit sous-corps de $\mathbb{R}$ contenant $x_1, \ldots, x_p, y_1, \ldots, y_p$ et stable par racine carrée ;
- si $t \in \mathbb{R}$, alors $t \in \mathscr{C}_\mathcal{B}$ si et seulement s'il existe une tour d'extensions quadratiques $L_1 \subseteq \ldots \subseteq L_n$ telle que $L_1 = \mathbb{Q}(x_1, \ldots, x_p, y_1, \ldots, y_p)$, $L_n \subseteq \mathbb{R}$, et $t \in L_n$ (théorème de Wantzel généralisé) ;
- si $t \in \mathscr{C}_\mathcal{B}$, alors t est algébrique sur $\mathbb{Q}(x_1, \ldots, x_p, y_1, \ldots, y_p)$ et le degré de son polynôme minimal est une puissance de 2.

En résumé, si $\theta \in \mathbb{R}$, alors θ est trisectable si, et seulement si, $\cos(\theta/3) \in \mathscr{C}_\mathcal{B}$. Le théorème qui suit donne une caractérisation algébrique des angles trisectables.

Théorème 3.4. *Soit $\theta \in \mathbb{R}$ tel que l'angle $\widehat{\theta}$ soit constructible. Alors θ est trisectable si, et seulement si, le polynôme :*

$$P_\theta = 4X^3 - 3X - \cos\theta \in \mathbb{Q}(\cos\theta)[X]$$

est réductible sur $\mathbb{Q}(\cos\theta)$.

Démonstration. Si $\cos(\theta/3) \in \mathscr{C}_\mathcal{B}$, alors d'après le théorème de Wantzel généralisé, $\cos(\theta/3)$ est algébrique sur $\mathbb{Q}(\cos\theta, \sin\theta)$. Clairement, $\mathbb{Q}(\cos\theta) \subseteq \mathbb{Q}(\cos\theta, \sin\theta)$, et cette extension est de degré 1 ou 2 car $\sin\theta$ est racine du polynôme :

$$X^2 + 1 - \cos^2\theta \in \mathbb{Q}(\cos\theta)[X].$$

On en déduit que $\cos(\theta/3)$ est algébrique sur $\mathbb{Q}(\cos\theta)$, et que le degré de son polynôme minimal μ_θ est une puissance de 2. En particulier, $\mu_\theta \neq P_\theta$ car $\deg P_\theta = 3$, mais $\cos(\theta/3)$ est racine de P_θ. Ce dernier est donc réductible sur $\mathbb{Q}(\cos\theta)$.

Réciproquement, si P_θ est réductible sur $\mathbb{Q}(\cos\theta)$, alors $\cos(\theta/3)$ est racine d'un polynôme de degré 1 ou 2 de $\mathbb{Q}(\cos\theta)[X]$. Or, le point $M \in \Gamma$ associé à θ est par définition constructible, donc $\mathbb{Q}(\cos\theta, \sin\theta) \subseteq \mathscr{C}_\mathcal{B}$, et on sait que $\mathbb{Q}(\cos\theta) \subseteq \mathbb{Q}(\cos\theta, \sin\theta)$. Comme $\mathscr{C}_\mathcal{B}$ est un corps stable par racine carrée, $\cos(\theta/3) \in \mathscr{C}_\mathcal{B}$. □

3.3 Deux lemmes essentiels

Avec cette notion d'angles orientés, on observe qu'un polygone régulier à n côtés est constructible si, et seulement si, l'angle « élementaire » de mesure $2\pi/n$ est constructible, puisqu'on peut alors reporter l'angle à l'aide du compas $n-1$ fois sur Γ pour obtenir tous les sommets. C'est cette idée qui motive les deux prochains lemmes. Nous noterons dans toute la suite l'angle élémentaire :

$$\widehat{a}(\theta) = \frac{\widehat{2\pi}}{\theta}.$$

Lemme 3.5. *Soient $m, n \geq 1$ deux entiers premiers entre eux. Alors l'angle $\widehat{a}(mn)$ est constructible si, et seulement si, les angles $\widehat{a}(m)$ et $\widehat{a}(n)$ sont constructibles.*

Démonstration. Si $\widehat{a}(mn)$ est constructible, alors on peut construire :

$$\widehat{a}(m) = n \cdot \widehat{a}(mn) \quad \text{et} \quad \widehat{a}(n) = m \cdot \widehat{a}(mn)$$

en reportant avec le compas respectivement n fois et m fois la corde correspondant à $\widehat{a}(mn)$.

Réciproquement, si $\widehat{a}(m)$ et $\widehat{a}(n)$ sont constructibles, alors comme m et n sont premiers entre eux, l'identité de Bézout garantit l'existence de deux entiers u et v tels que $um + vn = 1$, de sorte que :

$$v \cdot \widehat{a}(m) + u \cdot \widehat{a}(n) = \widehat{a}(mn).$$

En reportant avec le compas, on peut construire $v \cdot \widehat{a}(m)$ et $u \cdot \widehat{a}(n)$, et la somme de deux angles constructibles est constructible. □

Lemme 3.6. *Soit $n \geq 3$ un entier dont la décomposition en facteurs premiers s'écrit :*

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}.$$

Alors le polygone régulier à n côtés est contructible si, et seulement si, chaque $\widehat{a}(p_k^{\alpha_k})$ est constructible.

Démonstration. On procède par récurrence et on applique le lemme 3.5 pour l'hérédité. □

3.4 Rappels sur les polynômes cyclotomiques et les racines de l'unité

Avant d'aller plus avant dans notre recherche de caractérisation des polygones constructibles à la règle et au compas, il s'impose de faire quelques rappels qui s'avèreront utiles pour la suite.

Définition 3.7. *Soit $q \geq 2$ un entier. Les racines complexes du polynôme $X^q - 1$ sont appelées* racines $q^{\text{èmes}}$ de l'unité*, et l'on note $\mathbb{U}_q$ leur ensemble.*

On note également :

$$\omega_q = \cos\left(\frac{2\pi}{q}\right) + i \sin\left(\frac{2\pi}{q}\right) \in \mathbb{U}_q.$$

Les autres racines $q^{\text{èmes}}$ de l'unité sont donc exactement les :

$$\omega_q^k = \cos\left(\frac{2k\pi}{q}\right) + i \sin\left(\frac{2k\pi}{q}\right).$$

Lorsque k est premier avec n, on dira que ω_q^k est une racine *primitive* $q^{\text{ème}}$ de l'unité.

Proposition 3.8. *Soit $q \geq 2$ un entier. Alors :*

- *l'ensemble $\mathbb{U}_q$ muni de la multiplication usuelle sur $\mathbb{C}$ forme un groupe cyclique ;*
- *si $k \in \{1, \ldots, n\}$ est premier avec n, alors ω_q^k engendre $\mathbb{U}_q$.*

Démonstration. Tout ceci se déduit de l'isomorphisme de groupes :

$$\begin{aligned} \mathbb{Z}/q\mathbb{Z} &\longrightarrow \mathbb{U}_q \\ \overline{k} &\longmapsto \omega_q^k \end{aligned}$$

et des propriétés bien connues du groupe cyclique $(\mathbb{Z}/q\mathbb{Z}, +)$. □

Proposition 3.9. *Soit $q \geq 2$ un entier. Alors ω_q est algébrique sur $\mathbb{Q}$ et son polynôme minimal est :*

$$\Phi_q = \prod_{\zeta \in \mu_q^*(\mathbb{C})} (X - \zeta)$$

où $\mu_q^*(\mathbb{C})$ désigne l'ensemble des racines primitives $q^{èmes}$ de l'unité.

Démonstration. Admis.[4] □

Définition 3.10. *On appelle* fonction indicatrice d'Euler *l'application φ définie par :*

$$\varphi(n) = \text{card}\left\{k \in \{1, \ldots, n\} \mid \text{pgcd}(k, n) = 1\right\}.$$

Proposition 3.11. *Soient p un nombre premier et $\alpha \geq 1$ un entier. Alors :*

$$\varphi\left(p^\alpha\right) = p^{\alpha-1}(p-1).$$

Démonstration. Puisque p est premier, les éléments de $\{1, \ldots, p^\alpha\}$ non premiers avec p^α sont exactement ceux qui sont divisibles par p, qui sont au nombre de $p^{\alpha-1}$. □

Proposition 3.12. *Soit $q \geq 2$ un entier. Alors le polynôme Φ_q est de degré $\varphi(q)$. En particulier :*

$$[\mathbb{Q}(\omega_q) : \mathbb{Q}] = \varphi(q).$$

Démonstration. Ceci découle de la définition de $\varphi(q)$ et des rappels de la section 2.1. □

3.5 Nombres de Fermat et constructibilité des polygones réguliers

Nous allons à présent tenter de caractériser, à l'aide des nombres de Fermat et des résultats de la section précédente, les polygones réguliers constructibles.

Proposition 3.13. *Pour tout $k \in \mathbb{N}$, l'angle $\widehat{a}(2^k)$ est constructible.*

Démonstration. On procède par récurrence sur k : il suffit de savoir construire une bissectrice pour l'hérédité, ce qui a déjà été fait dans la proposition 1.6. □

Définition 3.14. *Pour $k \in \mathbb{N}$, on appelle $k^{\text{ème}}$* nombre de Fermat *l'entier :*

$$F_k = 1 + 2^{2^k}.$$

Lorsque F_k est premier, on l'appelle nombre premier de Fermat.

On ne connaît actuellement que 5 nombres de Fermat qui sont premiers :

$$F_0 = 3 \quad ; \quad F_1 = 5 \quad ; \quad F_2 = 17 \quad ; \quad F_3 = 257 \quad ; \quad F_4 = 65\,537.$$

Fermat avait conjecturé que $F_5 = 2^{32} + 1$ était premier, avant que Leonhard Euler (1707–1783) ne prouve le contraire [San07] :

$$F_5 = 4\,294\,967\,297 = 641 \times 6\,700\,417.$$

La preuve de la prochaine proposition est assez copieuse. Nous ferons une démonstration complète et autonome, mais nous verrons que la réciproque est nettement plus facile à obtenir si l'on dispose du théorème de Galois.

[4] Le polynôme Φ_q est appelé *$q^{ème}$ polynôme cyclotomique*, et on peut montrer que $\Phi_q \in \mathbb{Z}[X]$. La preuve de son irréductibilité sur $\mathbb{Q}$ n'est pas facile. On pourra en trouver une version détaillée en cliquant ici.

Proposition 3.15. *Soient $p \geq 3$ un nombre premier et $\alpha \geq 1$ un entier. Les assertions suivantes sont équivalentes :*

(i) *l'angle $\widehat{a}(p^\alpha)$ est constructible ;*

(ii) *p est un nombre de Fermat et $\alpha = 1$.*

Démonstration. Supposons que $\widehat{a}(p^\alpha)$ soit constructible, et notons :

$$c = \cos\left(\frac{2\pi}{p^\alpha}\right).$$

Le réel c est donc également constructible, et d'après le résultat de Wantzel, il existe $m \in \mathbb{N}$ tel que :

$$[\mathbb{Q}(c) : \mathbb{Q}] = 2^m.$$

Nous noterons jusqu'à la fin de la démonstration :

$$\omega = \cos\left(\frac{2\pi}{p^\alpha}\right) + i\sin\left(\frac{2\pi}{p^\alpha}\right).$$

D'après les propositions 3.9 et 3.11, le degré du polynôme minimal de ω vaut $p^{\alpha-1}(p-1)$. Le complexe ω est donc algébrique de degré $p^{\alpha-1}(p-1)$, et $[\mathbb{Q}(\omega) : \mathbb{Q}] = p^{\alpha-1}(p-1)$. Par ailleurs :

$$\omega + \omega^{-1} = \omega + \overline{\omega} = 2\cos\left(\frac{2\pi}{q}\right).$$

Ceci montre que $c \in \mathbb{Q}(\omega)$ et que ω est algébrique de degré 2 sur $\mathbb{Q}(c)$, d'où :

$$[\mathbb{Q}(\omega) : \mathbb{Q}(c)] = 2.$$

De l'égalité $[\mathbb{Q}(\omega) : \mathbb{Q}] = [\mathbb{Q}(\omega) : \mathbb{Q}(c)]\,[\mathbb{Q}(c) : \mathbb{Q}]$, on tire alors $p^{\alpha-1}(p-1) = 2^{m+1}$. Comme p est premier et impair, on a nécessairement $\alpha = 1$, soit finalement :

$$p = 1 + 2^{m+1}.$$

Montrons maintenant que $m+1$ est bien une puissance de 2. Écrivons $m+1 = 2^k\lambda$, où $k \in \mathbb{N}$ et $\lambda \geq 1$ est un entier impair, de sorte que :

$$p = 1 + 2^{2^k\lambda} = 1 + \left(2^{2^k}\right)^\lambda$$

et λ étant impair, le polynôme $1 + X^\lambda$ est divisible par $1 + X$, donc $1 + 2^{2^k}$ divise p. Or, p est premier donc $\lambda = 1$, c'est-à-dire $p = F_k$.

La démonstration de la réciproque nécessite de nous attarder sur quelques résultats intermédiaires. Supposons que p soit un nombre premier de Fermat de la forme $p = 1 + 2^n$ avec $n \geq 1$. On note à présent $K = \mathbb{Q}(\omega)$.

1. Une base de K sur $\mathbb{Q}$. Notons que toutes les racines $p^{\text{èmes}}$ de l'unité différentes de 1 sont primitives. Par définition, $[K : \mathbb{Q}]$ est le degré du polynôme minimal de ω sur $\mathbb{Q}$. D'après les propositions 3.9 et 3.11, c'est :

$$\Phi_p = X^{p-1} + \ldots + X + 1.$$

Par conséquent, $[K : \mathbb{Q}] = p - 1$ et $(1, \omega, \ldots, \omega^{p-2})$ est une base de K sur $\mathbb{Q}$ (cf. section 2.1).

2. Automorphismes de K. On note G le groupe des automorphismes de K, dont on cherche à déterminer les éléments. On remarque que si $g \in G$, alors $g(1) = 1$ et on déduit successivement des propriétés des morphismes de corps que g laisse invariant $\mathbb{N}$, $\mathbb{Z}$ puis $\mathbb{Q}$. En particulier, g est entièrement déterminé par $g(\omega)$. De l'égalité $\Phi_p(\omega) = 0$, on tire :

$$g(\omega)^{p-1} + \ldots + g(\omega) + 1 = 0.$$

Donc $g(\omega)$ est racine de μ_ω, dont les racines sont exactement les racines $p^{\text{èmes}}$ de l'unité différentes de 1. Par conséquent, $g(\omega) \in \{\omega, \omega^2 \dots, \omega^{p-1}\}$. On admettra alors le petit lemme suivant.

Lemme 3.16. *Si M/L est une extension de corps, et $a, b \in M$ ont même polynôme minimal sur L, alors il existe un isomorphisme de corps $\sigma : L(a) \to L(b)$ tel que $\sigma(a) = b$, et $\sigma(\ell) = \ell$ pour tout $\ell \in L$.*

Comme les ω^k $(1 \leq k \leq p-1)$ sont des racines primitives $p^{\text{èmes}}$ de l'unité, leur polynôme minimal est Φ_p. Puisque $K = \mathbb{Q}(\omega) = \mathbb{Q}(\omega^k)$, les isomorphismes donnés par le lemme 3.16 sont en fait des automorphismes de K et nous permettent d'écrire $G = \{g_1, \dots, g_{p-1}\}$ avec pour tout $k \in \{1, \dots, p-1\}$, $g_k(\omega) = \omega^k$.

3. Structure de groupe cyclique. Comme $\mathbb{F}_p^\times$ est un groupe cyclique, on montre que l'application :

$$\begin{aligned} G &\longrightarrow \mathbb{F}_p^\times \\ g_k &\longmapsto \overline{k} \end{aligned}$$

est un isomorphisme de groupes, donc G est également cyclique. On notera g l'un de ses générateurs.

4. Une autre base de K. On vérifie que $(\omega, \omega^2, \dots, \omega^{p-1})$ est également une base de K sur $\mathbb{Q}$. Quitte à permuter ses éléments, on obtient la base $(g(\omega), \dots, g^{p-1}(\omega))$ ou encore $B = (\omega, g(\omega), \dots, g^{p-2}(\omega))$.

5. Une suite croissante de corps. On avait posé $p = 1 + 2^n$, donc G est cyclique de cardinal 2^n et g est d'ordre 2^n. De plus, pour tout $i \in \{1, \dots, n\}$, g^i est d'ordre 2^{n-i}. En notant G_i le sous-groupe de G engendré par g^i, qui est donc d'ordre 2^{n-i}, on obtient une suite strictement croissante de sous-groupes :

$$\{\mathrm{id}\} = G_n \subsetneq G_{n-1} \subsetneq \cdots \subsetneq G_0 = G.$$

On associe à cette suite de sous-groupes une suite de sous-corps de K, en posant, pour tout $i \in \{0, \dots, n\}$:

$$K_i = \left\{ z \in K \;\middle|\; g^{2^i}(z) = z \right\}$$

Pour tout $i \in \{0, \dots, n-1\}$, $K_i \subseteq K_{i+1}$ car $g^{2^{i+1}} = \left(g^{2^i}\right)^2$. On a donc $K_0 \subseteq \cdots \subseteq K_n = K$.

6. Description de K_0. Montrons que $K_0 = \mathbb{Q}$. On a tout d'abord $\mathbb{Q} \subseteq K_0 = \{z \in K \mid g(z) = z\}$, d'après les résultats sur les automorphismes de K. Soit maintenant $z \in K_0$. On décompose z dans la base B :

$$z = \lambda_0 \omega + \lambda_1 g(\omega) + \ldots + \lambda_{p-2} g^{p-2}(\omega)$$

où $\lambda_0, \dots, \lambda_{p-2} \in \mathbb{Q}$. Ainsi :

$$g(z) = \lambda_0 g(\omega) + \lambda_1 g^2(\omega) + \ldots + \lambda_{p-2} g^{p-1}(\omega) = \lambda_0 g(\omega) + \lambda_1 g^2(\omega) + \ldots + \lambda_{p-2}(\omega).$$

Or, $g(z) = z$ par définition de K_0, donc $\lambda_0 = \lambda_1 = \ldots = \lambda_{p-2}$. De plus :

$$\omega + g(\omega) + \ldots + g^{p-2}(\omega) = \omega + \omega^2 + \ldots + \omega^{p-1} = -1$$

car la somme des racines $p^{\text{èmes}}$ de l'unité est nulle. Par conséquent, $z = -\lambda_0 \in \mathbb{Q}$, et ceci pour tout $z \in K_0$.

7. Tour d'extensions. Montrons que pour tout $i \in \{1, \dots, n-1\}$, $K_i \subsetneq K_{i+1}$. Il suffit donc de trouver $z \in K$ tel que $g^{2^{i+1}}(z) = z$ et $g^{2^i}(z) \neq z$. Montrons d'abord que $K_0 \subsetneq K_1$. Pour ce faire, on pose :

$$z = \omega + g^2(\omega) + g^4(\omega) + \ldots + g^{2^n - 2}(\omega).$$

On constate alors que :

$$g^2(z) = g^2(\omega) + g^4(\omega) + \ldots + g^{2^n-2}(\omega) + g^{2n}(\omega) = g^2(\omega) + g^4(\omega) + \ldots + g^{2^n-2}(\omega) + \omega = z$$

et en g, il vient :

$$g(z) = g(\omega) + g^3(\omega) + g^5(\omega) + \ldots + g^{2^n-1}(\omega).$$

Par unicité de la décomposition de z dans la base B, on constate que $g(z) \neq z$. Le cas général se démontre de manière analogue, en considérant :

$$z = \omega + g^{2^{i+1}}(\omega) + \ldots + g^{2^{i+1}\left(2^{n-i-1}-1\right)}(\omega).$$

En résumé, on dispose d'une tour d'extensions :

$$\mathbb{Q} = K_0 \subsetneq K_1 \subsetneq \ldots \subsetneq K_n = K.$$

8. Description de K_{n-1}. Notons temporairement :

$$c = \cos\left(\frac{2\pi}{p}\right)$$

et montrons que $K_{n-1} = \mathbb{Q}(c)$. On considère $\lambda \in \mathbb{N}$ tel que $g^{2^{n-1}}(\omega) = \omega^\lambda$. De l'égalité $g^{2^n} = 1$, on tire :

$$\omega = \left(g^{2^{n-1}}\right)^2(\omega) = g\left(\omega^\lambda\right) = \omega^{\lambda^2}$$

d'où $\omega^{\lambda^2-1} = 1$. Donc par le théorème de Lagrange, p divise $\lambda^2 - 1$, puis $\lambda \equiv \pm 1 \pmod p$. Puisque $g^{2^{n-1}} \neq 1$, on a nécessairement $\lambda \equiv -1 \pmod p$, et cela entraîne :

$$g^{2^{n-1}}(\omega) = \omega^{-1}.$$

In fine :

$$g^{2^{n-1}}\left(\cos\left(\frac{2\pi}{p}\right)\right) = g^{2^{n-1}}\left(\frac{\omega+\omega^{-1}}{2}\right) = \frac{1}{2}\,g^{2^{n-1}}\left(\omega+\omega^{-1}\right) = \frac{\omega+\omega^{-1}}{2} = \cos\left(\frac{2\pi}{p}\right)$$

donc $\mathbb{Q}(c) \subseteq K_{n-1}$, car tous les rationnels sont également des points fixes. Par ailleurs, nous avons vu dans la preuve du sens direct que :

$$[K : \mathbb{Q}(c)] = [\mathbb{Q}(\omega) : \mathbb{Q}(c)] = 2$$

et comme $K_{n-1} \neq K$, on obtient finalement :

$$\mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right) = K_{n-1}.$$

9. Fin de la preuve. Avec notre tour d'extensions $\mathbb{Q} = K_0 \subsetneq \ldots \subsetneq K_n = K = \mathbb{Q}(\omega)$, on a donc :

$$2^n = p - 1 = [K : \mathbb{Q}] = [K : K_{n-1}] \cdots [K_1 : K_0]\,.$$

Ce dernier produit comporte n facteurs entiers, tous supérieurs ou égaux à 2 car les inclusions sont strictes, et ce sont des diviseurs de 2^n. Ils valent donc tous 2 par le principe des tiroirs. Enfin, la suite de corps :

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_{n-1} = \mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right)$$

forme une tour d'extensions quadratiques. Le théorème de Wantzel couplé à la proposition 3.2 permettent de conclure. □

Théorème 3.17 (Gauss). *Soit $n \geq 3$ un entier. Alors le polygone régulier à n côtés est constructible si, et seulement si, n est le produit d'une puissance de 2 et de nombres premiers de Fermat.*

Démonstration. Découle directement du lemme 3.6 et des propositions 3.13 et 3.15. □

4 Compléments

4.1 Extension aux nombres complexes

La notion de constructibilité dans $\mathbb{C}^2$, c'est-à-dire dans $\mathbb{R}^4$, n'est pas vraiment propice à l'intuition, mais on peut tout de même généraliser le théorème 2.5.

Théorème 4.1. *L'ensemble $\mathscr{C}(i)$ est le plus petit sous-corps de $\mathbb{C}$ stable par racine carrée.*

Démonstration. Montrons tout d'abord que $\mathscr{C}(i)$ est stable par racine carrée. Puisque $i^2 = -1 \in \mathscr{C}$:

$$\mathscr{C}(i) = \{a + ib \mid a, b \in \mathscr{C}\}.$$

Soient $z = a + ib \in \mathscr{C}(i)$ et $u, v \in \mathbb{R}$ tels que $(u + iv)^2 = z$. Montrons que $u, v \in \mathscr{C}$. On sait déjà que :

$$\begin{cases} u^2 - v^2 = a \\ u^2 + v^2 = |z| = \sqrt{a^2 + b^2} \end{cases}$$

ce qui nous permet, aux signes près, d'expliciter u et v :

$$u = \pm\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}} \quad ; \quad v = \pm\sqrt{\frac{\sqrt{a^2+b^2}-a}{2}}$$

les signes étant déterminés par la condition $2uv = b$. Dans tous les cas, $u, v \in \mathscr{C}$ d'après le théorème 1.10.

Montrons à présent que $\mathscr{C}(i)$ est le plus petit sous-corps de $\mathbb{C}$ vérifiant cette propriété de stabilité. Si K est un sous-corps de $\mathbb{C}$ stable par racine carrée, alors $K \cap \mathbb{R}$ est un sous-corps de $\mathbb{R}$ stable par racine carrée. D'après le théorème 2.5, $\mathscr{C} \subseteq K \cap \mathbb{R} \subseteq K$. De plus, $-1 \in K$ donc $i \in K$, ce qui donne finalement $\mathscr{C}(i) \subseteq K$. □

4.2 Construction par neusis

On peut se demander si les outils à notre disposition n'étaient pas trop limités. Par exemple, quels points du plan peut-on atteindre si l'on ajoute deux graduations sur la règle ? C'est le principe de la construction par *neusis* (du grec ancien $\nu\varepsilon\upsilon\varepsilon\iota\nu$, « inclinaison »), qui consiste à placer un segment de longueur fixée entre deux courbes, de sorte que la droite sur lequel s'appuie le segment passe toujours par le même point.

On suppose désormais que la règle comporte deux graduations distantes d'une unité. On dira qu'un point M est *constructible par neusis* lorsqu'il est possible de faire glisser ou pivoter la règle de sorte que celle-ci passe toujours par un point constructible fixé P, pendant que l'une des graduations parcourt un cercle-droite constructible, et que le point M se situe au niveau de la seconde graduation à la fin de la manipulation. On dira enfin qu'un nombre réel est *constructible par neusis* lorsque c'est l'une des coordonnées d'un point constructible par neusis.

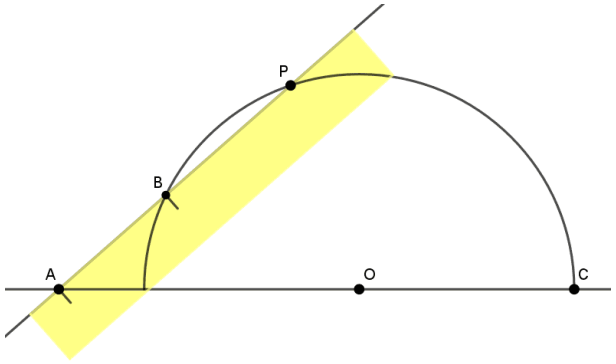


FIGURE 11 – Illustration de la construction avec une règle graduée.

Dans l'exemple ci-dessus, le point P est fixé pendant que A parcourt la droite (OC). Une fois la deuxième graduation au niveau du demi-cercle Γ^+, on obtient le point B. On pourrait penser que tout cela est superflu, mais nous allons voir qu'il n'en est rien, puisque deux des trois problèmes deviennent résolubles.

Trisection de l'angle. Voici une construction due à Archimède. Positionnons la première graduation de la règle sur l'axe des abscisses, tout en faisant passer la règle par le point M. Construisons le point A tel que la seconde graduation soit sur le demi-cercle Γ^+ et que le point B au niveau de cette graduation vérifie $AB = 1$.

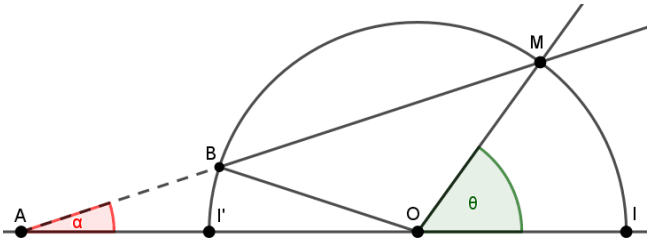


FIGURE 12 – Trisection d'un angle θ quelconque en α.

Montrons que $\alpha = \theta/3$. Remarquons que le triangle OAB est isocèle en B, donc $\widehat{AOB} = \alpha$, puis $\widehat{OBM} = 2\alpha$. Le triangle OBM est par ailleurs isocèle en O, donc $\widehat{OMB} = 2\alpha$. Par conséquent :

$$\widehat{OMB} + \widehat{MBO} + \widehat{BOM} = 4\alpha + \pi - \alpha - \theta = \pi$$

soit exactement $\alpha = \theta/3$. Il suffisait donc de deux graduations pour qu'une méthode générale apparaisse.

Duplication du cube. Il existe de très nombreuses façons de procéder, en voici une qui fait appel au *théorème de Ménélaüs*. Ce dernier stipule que si ABC est un triangle, et si $D \in (BC)$, $E \in (AC)$ et $F \in (AB)$, alors les points D, E et F sont alignés si, et seulement si :

$$\frac{DB}{DC}\frac{EC}{EA}\frac{FA}{FB} = 1$$

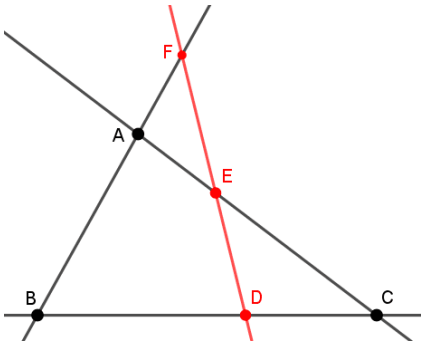


FIGURE 13 – Illustration du théorème de Ménélaüs.

On construit tout d'abord le point A d'ordonnée positive tel que OIA soit équilatéral. On positionne ensuite la règle graduée sur $[OA]$ avec la deuxième graduation en O, et on obtient un point $B \in (OA)$ tel que $OB = 1$. On trace ensuite la droite (BI), et on positionne la règle graduée sur A avec la première graduation sur l'axe des abscisses. Lorsque la deuxième graduation atteint (BI), on obtient alors deux points C et D tels que $CD = 1$.

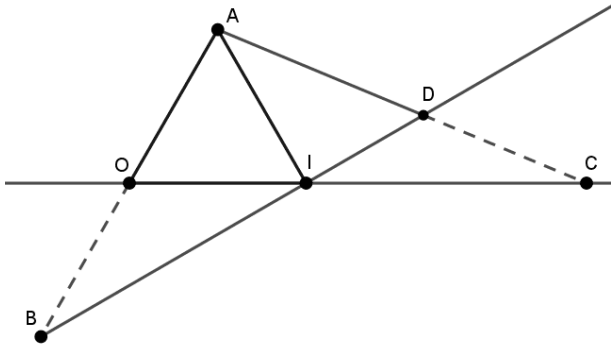


FIGURE 14 – Construction d'un segment de longueur $\sqrt[3]{2}$.

Montrons que $AD = \sqrt[3]{2}$. Notons $\alpha = \widehat{OAI} = \pi/3$ et $\beta = \widehat{OBI}$. Puisque le triangle OBI est isocèle en O :

$$\widehat{OBI} + \widehat{OIB} + \widehat{IOB} = 2\beta + \pi - \alpha = \pi$$

donc $\beta = \alpha/2 = \pi/6$, puis :

$$\widehat{AIB} = \widehat{AIO} + \widehat{OIB} = \frac{\pi}{2}.$$

Le triangle AIB est donc rectangle en I. En vertu du théorème de Pythagore :

$$IB = \sqrt{AB^2 - AI^2} = \sqrt{3}.$$

Puisque les points $B \in (OA)$, $I \in (OC)$ et $D \in (AC)$ sont alignés, d'après le théorème de Ménélaüs appliqué au triangle OAC :

$$\frac{BO}{BA}\frac{IC}{IO}\frac{DA}{DC} = 1$$

c'est-à-dire $AD = 2/IC$. Par ailleurs, les points $O \in (AB)$, $I \in (BD)$ et $C \in (AD)$ sont également alignés, donc le théorème de Ménélaüs appliqué cette fois au triangle ABD donne :

$$\frac{OA}{OB}\frac{IB}{ID}\frac{CD}{CA} = 1$$

ce dont on déduit :

$$AD + 1 = AC = \frac{OA \times IB \times CD}{OB \times ID} = \frac{\sqrt{3}}{ID} = \frac{\sqrt{3}}{\sqrt{AD^2 - 1}}.$$

En résumé, AD est racine du polynôme :

$$(X+1)^2\left(X^2-1\right) - 3 = X^4 + 2X^3 - 2X - 4 = (X+2)\left(X^3 - 2\right)$$

et c'est un réel strictement positif, donc $AD = \sqrt[3]{2}$.

Quadrature du cercle. Nous admettrons le théorème suivant [Bar02].

Théorème 4.2 (Baragar, 2002). *Soit $t \in \mathbb{R}$. Si t est constructible par neusis, alors il existe une tour d'extensions $L_1 \subseteq \ldots \subseteq L_n$ telle que $L_1 = \mathbb{Q}$, $t \in L_n \subseteq \mathbb{R}$ et pour tout $i \in \{1, \ldots, n-1\}$, $[K_{i+1} : K_i] \leq 6$.*

En particulier, la quadrature du cercle reste impossible puisque les longueurs constructibles par neusis sont nécessairement algébriques.

Polygones réguliers. Il devient possible de construire le polygone régulier à n côtés pour $n = 7$, 9, 13, 14, 18, 19, 21, 26, 27, 28, 35, 36, 37, 38, 39, 42, 52, 54, 56, 57, 63, 65, 70, 72, 73, 74, 76, 78, 81, 84, 91, 95, 97, 104, 105, 108, 109, 111, 112, 114, 117, 119. On sait par ailleurs depuis 2014 que le polygone régulier à 11 côtés est constructible par neusis [ES14]. Le problème reste ouvert pour $n \in \{25, 31, 41, 61, 101, 125\}$, et plus généralement pour $n = 5^k$ avec $k \geq 2$, et pour les nombres premiers de la forme $n = 2^k 3^\ell 5^m + 1$ avec $m \geq 1$.

4.3 Vers la théorie de Galois

Nous présentons sans démonstration quelques résultats fondamentaux concernant la théorie de Galois, que l'on se contentera d'effleurer ici, afin de retrouver la caractérisation des polygones réguliers constructibles.

4.3.1 Quelques définitions

Définition 4.3. *Soient L/K une extension de corps et $\sigma : L \to L$ un automorphisme de corps. On dit que σ est un* K-automorphisme de L *lorsque $\sigma(k) = k$ pour tout $k \in K$.*

Si $K = \mathbb{R}$ et $L = \mathbb{C}$, c'est par exemple le cas de la conjugaison $\sigma_{\mathbb{C}}(z) = \overline{z}$.

Définition 4.4. *Soit L/K une extension de corps. On note* $\mathrm{Gal}(L/K)$ *et on appelle* groupe de Galois *de cette extension le groupe des K-automorphismes de L.*

L'exemple précédent montre que $\{\mathrm{id}_{\mathbb{C}}, \sigma_{\mathbb{C}}\} \subseteq \mathrm{Gal}(\mathbb{C}/\mathbb{R})$. Nous pouvons d'ores et déjà montrer que c'est une égalité. En effet, si φ est un $\mathbb{R}$-automorphisme de $\mathbb{C}$, alors de l'égalité $i^2 + 1 = 0$, on tire :

$$\varphi(i)^2 + 1 = 0$$

donc $\varphi(i) \in \{-i, i\}$. Comme $\varphi(i)$ détermine entièrement φ, on en déduit $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}_{\mathbb{C}}, \sigma_{\mathbb{C}}\}$.

4.3.2 Correspondances entre sous-groupes et sous-corps

Considérons une extension de corps L/K. Dans toute la suite, on notera :

- $\mathcal{M}_{L/K}$ l'ensemble des corps M tels que $K \subseteq M \subseteq L$, appelés *corps intermédiaires* de l'extension ;
- $\mathcal{H}_{L/K}$ l'ensemble des sous-groupes de $\mathrm{Gal}(L/K)$;

et si $M \in \mathcal{M}_{L/K}$ et $H \in \mathcal{H}_{L/K}$, on notera :

- M° l'ensemble des éléments de $\mathrm{Gal}(L/K)$ laissant invariant chaque élément de M ;
- H^* l'ensemble des éléments de L invariants par tout élément de H.

Proposition 4.5. *Si $M, M' \in \mathcal{M}_{L/K}$ et $H, H' \in \mathcal{H}_{L/K}$, alors :*

(i) *M° est un sous-groupe de* $\mathrm{Gal}(L/K)$*, c'est* $\mathrm{Gal}(L/M)$ *;*

(ii) *H^* est un corps intermédiaire, appelé* corps fixe *de H ;*

(iii) *$M \subseteq M'$ entraîne $(M')^\circ \subseteq M^\circ$;*

(iv) *$H \subseteq H'$ entraîne $(H')^* \subseteq H^*$;*

(v) *$M \subseteq (M^\circ)^*$;*

(vi) *$H \subseteq (H^*)^\circ$.*

4.3.3 Extensions normales et théorème de Galois

Définition 4.6. *Une extension de corps L/K est dite* normale *lorsque tout polynôme irréductible à coefficients dans K qui possède une racine dans L est scindé sur L.*

C'est par exemple le cas de l'extension $\mathbb{C}/\mathbb{R}$, la deuxième condition étant toujours vérifiée d'après le théorème fondamental de l'algèbre.

Proposition 4.7. *Une extension de corps L/K est normale et de degré fini si, et seulement si :*

$$L = K(\alpha_1, \alpha_2, \dots, \alpha_r)$$

où $\alpha_1, \dots, \alpha_r$ sont les racines dans L d'un certain polynôme de $K[X]$ scindé sur L.

Théorème 4.8 (Galois). *Soient K un corps de caractéristique nulle et L/K une extension normale de degré fini $n \in \mathbb{N}$. Alors :*

(i) *le groupe $\mathrm{Gal}(L/K)$ est fini d'ordre n ;*

(ii) *les applications $*$ et $\circ$ sont décroissantes pour l'inclusion, bijectives et réciproques l'une de l'autre (correspondances de Galois) ;*

(iii) *si M est un corps intermédiaire, alors l'extension M/K est normale si, et seulement si, M° est un sous-groupe distingué de $\mathrm{Gal}(L/K)$; si de plus ces conditions sont remplies, alors :*

$$\mathrm{Gal}(M/K) \cong \mathrm{Gal}(L/K) \,/\, \mathrm{Gal}(L/M).$$

4.3.4 Retour au problème des polygones réguliers

L'étude du groupe $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ va nous permettre de démontrer la proposition 3.15 plus facilement, à l'aide des résultats précédents. On établit d'abord que les hypothèses du théorème de Galois sont vérifiées.

Proposition 4.9. *Si $n \in \mathbb{N}^*$ et ω_n est une racine primitive $n^{\text{ème}}$ de l'unité, alors l'extension $\mathbb{Q}(\omega_n)/\mathbb{Q}$ est normale et de degré fini.*

Démonstration. On sait que $\mathbb{Q}(\omega_n) = \mathbb{Q}(1, \omega_n, \dots, \omega_n^{n-1})$, et les ω_n^k sont les racines dans $\mathbb{Q}(1, \omega_n, \dots, \omega_n^{n-1})$ du polynôme $X^n - 1 \in \mathbb{Q}[X]$ qui est de degré n. □

Nous avions établi que si ω est une racine $p^{\text{ème}}$ de l'unité, alors :

$$\mathrm{Aut}(\mathbb{Q}(\omega)) \cong \mathbb{F}_p^\times.$$

Or, nous savons que si $\varphi \in \mathrm{Aut}(\mathbb{Q}(\omega))$, alors $\varphi(q) = q$ pour tout $q \in \mathbb{Q}$, donc d'après le théorème de Galois :

$$\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong \mathbb{F}_p^\times.$$

4.3.5 Nouvelle démonstration du théorème de Gauss

Nous sommes maintenant en mesure de redémontrer la proposition 3.15 de manière nettement plus concise. La preuve du sens direct est identique. Pour la réciproque, notant ω une racine primitive $p^{\text{ème}}$ de l'unité, la proposition 4.9 assure que l'extension $\mathbb{Q}(\omega)/\mathbb{Q}$ est normale et de degré fini, et nous avons vu que $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2^n$ pour un certain entier $n \geq 1$. Ainsi, d'après le théorème de Galois :

$$|\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})| = 2^n.$$

De plus, $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ est isomorphe à $\mathbb{F}_p^\times$ donc est cyclique. Considérons-en un générateur g, et notons H_i le groupe engendré par g^{2^i}. Les H_i sont exactement les sous-groupes de $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$, et :

$$\{\mathrm{id}\} = H_n \subseteq \cdots \subseteq H_0 = \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}).$$

On note à présent $K_i = H_i^*$ pour $i \in \{0, \dots, n\}$, de sorte que :

$$\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})^* = K_0 \subseteq \cdots \subseteq K_n = \{\mathrm{id}\}^*.$$

Par correspondance de Galois, $K_0 = \mathbb{Q}$ et $K_n = \mathbb{Q}(\omega)$. Il reste alors à montrer que c'est une tour d'extensions quadratiques. Comme $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ est cyclique, il est en particulier abélien donc tous ses sous-groupes sont distingués. Ainsi, K_i° est distingué dans $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ et d'après le théorème de Galois :

$$\mathrm{Gal}(K_i/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \,/\, \mathrm{Gal}(\mathbb{Q}(\omega)/K_i).$$

Enfin, par définition :

$$\mathrm{Gal}(\mathbb{Q}(\omega)/K_i) = K_i^\circ = (H_i^*)^\circ = H_i$$

et puisque K_i° est distingué, l'extension $K_i/\mathbb{Q}$ est normale et de degré fini. Par conséquent :

$$[K_i : \mathbb{Q}] = |\mathrm{Gal}(K_i/\mathbb{Q})| = \frac{|\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})|}{|\mathrm{Gal}(\mathbb{Q}(\omega)/K_i)|} = \frac{[\mathbb{Q}(\omega) : \mathbb{Q}]}{|H_i|} = \frac{2^n}{2^{n-i}} = 2^i$$

et on conclut de la même façon que dans la preuve précédente de ce résultat.

Au-delà des polygones réguliers, signalons que l'on peut également montrer le résultat suivant, qui achève la caractérisation des nombres réels constructibles à la règle non graduée et au compas.

Théorème 4.10. *Soit $t \in \mathbb{R}$. Alors t est constructible si, et seulement si, t est algébrique sur $\mathbb{Q}$ et le degré du corps de décomposition du polynôme minimal de t sur $\mathbb{Q}$ est une puissance de 2.*

Bibliographie

[Bar02] A. Baragar, « Constructions Using a Compass and Twice-Notched Straightedge », *The American Mathematical Monthly*, vol. 109, no. 2, 2002, pp. 151–164.

[Car89] J.-C. Carrega, *Théorie des corps – La règle et le compas*, 1989.

[ES14] B. Elliot, C. Snyder, *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 156, no. 3, 2014, pp. 409–424.

[Lin82] F. Lindemann, « Über die Zahl π », *Math. Ann.*, vol. 20, 1882, pp. 213–225.

[San07] E. Sandifer, « How Euler did it – Factoring F_5 », 2007, sur `https://ghostarchive.org/archive/0UUFo`.

[Wan37] L. Wantzel, « Recherches sur les moyens de reconnaître si un Problème de Géométrie peut se résoudre avec la règle et le compas », *J. Math. Pures Appl.*, série n°1, vol. 2, 1837, pp. 366–372.